Algoritmi za prostotu grupa pomoću teorema Silova

Žarko Bulić
zarkovaSrednja
e-mail: ZarkovEmail

Pavle Tepavčevic
PMF Novi Sad
e-mail: PavlovEmail

Mateja Vuković
Gimnazija "Jovan Jovanović Zmaj"
e-mail: vukovic.mateja@jjzmaj.edu.rs

12.11.2020.

Apstrakt

Pojam proste grupe uveo je 1832. godine Evarist Galoa. Četrdeset godina kasnije, norveški matematičar Ludvig Silov objavio je tri teoreme koje na osnovu reda grupe garantuju postojanje određenih podgrupa. Cilj ovog rada jeste da, služeći se teoremama Silova, za zadat prirodan broj n odgovori na pitanje: "Da li postoji prosta grupa reda n". U radu smo se fokusirali na brojeve n određenog oblika i ostavili prostora za dalje istraživanje na ovu temu.

Apstrakt

Simple groups were first introduced in 1832. by Évariste Galois. Forty years later, Norwegian mathematician Ludwig Sylow published three theorems which, based on the order of a finite group, guaranteed the existence of specific subgroups to that particular group. The goal of this paper is to answer the question "Are there any simple groups of order n"?, for a given positive integer n. We focused on numbers n of a certain type, partially answering the posed question and leaving space for further research on this topic.

1 Teorijski uvod

1.1 Grupe

Grupe jesu jedna od danas najproučavanijih algebarskih struktura. Njihova pojava u matematici omogućila je rešavanje brojnih problema koji su do tada bili otvoreni. U ovom poglavlju navodimo samo par elementarnih pojmova i teorema vezanih za grupe.

Definicija 1.1 *Algebarska struktura $(G, +)$ naziva se grupa ako i samo ako važi:*

- *Postoji element e takav da za svako $x \in G$ važi $x + e = e + x = x$,*
- *Za svako $x, y, z \in G$ važi $(x + y) + z = x + (y + z)$,*
- *Za svako x postoji y takvo da važi $x + y = y + x = e$.*

Dakle, možemo reći da je grupa algebarska struktura koja ima neutralni element, asocijativna je i svaki element unutar nje je invertibilan(postoji neki drugi element koji daje neutral kada učestvuje u operaciji sa prvim elementom). U prevodu, grupa je monoid unutar koga su svi elementi invertibilni.

Primer 1.1 $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, \cdot)$ *su grupe, dok* $(\mathbb{N}, +)$ *nije grupa jer nema svaki element svog inverza.*

Teorema 1.2 *Neka je $(G, \cdot)$ grupa i neka su g i h elemneti takvi da važi $gh = hg = 1$. Tada je element h jedinstven za element g(i obratno), i takav element se naziva inverzom elemnta g.*

Dokaz. Pretpostavimo da postoje dva elementa, $h_1, h_2 \in G$ takva da važi $gh_1 = h_1 g = 1$ i $gh_2 = h_2 g = 1$. Tada važi $h_1 = h_1 \cdot 1 = h_1(gh_2) = (h_1 g)h_2 = 1 \cdot h_2 = h_2$, odakle sledi jedinstvenost ovakvog elementa.■

Napomena: Često ćemo inverzni elemenat elementa g označavati sa g^{-1}.

Definicija 1.3 *Ako je $(G, \cdot)$ grupa, onda se kardinalnost skupa G naziva redom grupe $(G, \cdot)$.*

Definicija 1.4 *Ukoliko je operacija $+$ unutar grupe $(G, +)$ komutativna, onda je ta grupa Abelova grupa.*

Teorema 1.5 *Neka je $(G, \cdot)$ grupa. Tada važe sledeće formule:*

- $xa = ya \Rightarrow x = y$,
- $ax = ay \Rightarrow x = y$,
- $(a^{-1})^{-1} = a$,
- $(ab)^{-1} = b^{-1}a^{-1}$.

Dokaz. Prvo tvrđenje dokazujemo tako što ćemo obe strane pomnožiti sa desne strane sa a^{-1}. Dobijamo $xa(a^{-1}) = ya(a^{-1})$, što je ekvivalentno sa $xe = ye$ odnosno $x = y$. Drugo tvrđenje pokazujemo analogno. Treće tvrđenje sledi iz $(a^{-1})^{-1} = (a^{-1})^{-1}e = (a^{-1})^{-1}(a^{-1}a) = ((a^{-1})^{-1}a^{-1})a = ea = a$. Četvrto tvrđenje sledi iz $(ab)^{-1} = (ab)^{-1}e = (ab)^{-1}aa^{-1} = (ab)^{-1}aea^{-1} = (ab)^{-1}abb^{-1}a = ((ab)^{-1}ab)b^{-1}a = eb^{-1}a = b^{-1}a$. ■

1.2 Podgrupa

Definicija 1.6 *Ako je $(G,\cdot)$ grupa, i H neki neprazan podskup skupa G takav da je $(H,\cdot|_{H^2})$ grupa, onda takvu strukturu nazivamo podgrupom grupe $(G,\cdot)$ i pišemo $(H,\cdot|_{H^2}) \prec (G,\cdot)$.*

Napomena: U nastavku ćemo podrazumevati da operaciju unutar podgrupe posmatramo na domenu te podgrupe(izostavljaćemo indeks uz oznaku za operaciju) Primetimo da je trivijalna grupa podgrupa svake grupe, kao i da je svaka grupa samoj sebi podgrupa. Ove dve podgrupe se nazivaju *trivijalne podgrupe*. Ako je nosač podgrupe pravi podskup nosača grupe, tada tu podgrupu nazivamo *pravom podgrupom*.

Teorema 1.7 *Ako je $(G,\cdot)$ grupa, onda je neprazni podskup H skupa G nosač podgrupe ako i samo ako za svako $a,b \in H$ važi $ab \in H$ i $a^{-1} \in H$.*

Dokaz. Ako H jeste nosač podgrupe, tada navedene osobine slede iz definicije grupe. Ostaje da pokažemo drugi smer. Asocijativnost operacije svakako važi jer ona važi na celom skupu G, pa samim tim i na svim njegovim podskupovima. Uslov zatvorenosti operacije i postojanja inverza kod svakog elementa su direktne posledice uslova. Ostaje da pokažemo da postoji neutralni element. Odaberimo neki element $a \in H$. Iz uslova je i $a^{-1} \in H$, pa je i $aa^{-1} = e \in H$. ■

Definicija 1.8 *Neka je $(G,\cdot)$ grupa i $(H,*)$ neka njena podgrupa. Ako je $g \in G$, onda je leva klasa elementa g s obzirom na podgrupu H skup $gH = \{gh|h \in H\}$. Analogno se definiše i desna klasa elementa g s obzirom na podgrupu H.*

Definicija 1.9 *Podgrupa $(H,*)$ je normalna podgrupa grupe $(G,*)$, u oznaci $(H,*) \lhd (G,*)$, ako i samo ako je $(H,*) \prec (G,*)$ i za svako $x \in G$ važi $xH = Hx$.*

Pored ove definicije, normalna podgrupa se često definiše i na sledeći način.

Definicija 1.10 *Podgrupa H grupe G je normalna ako i samo ako $(\forall g \in G)(gHg^{-1} = H)$.*

Teorema 1.11 *Ako je G grupa a H njena normalna podgrupa G/H je Abelova ako i samo ako $(\forall g_1, g_2 \in G)(g_1^{-1}g_2^{-1}g_1g_2 \in H)$*

Dokaz. ($\Longrightarrow$) Pretpostavimo da je G/H Abelova grupa. Neka su $g_1, g_2 \in G$. Onda $g_1H, g_2H \in G/H$ a s obzirom na to da je G/H Abelova imamo:

$$(g_1H)(g_2H) = (g_2H)(g_1H)$$

Kako je $(g_1H)(g_2H) = (g_1g_2H)$ i $(g_2H)(g_1H) = (g_2g_1H)$ imamo da:

$$g_1g_2H = g_2g_1H$$

$$g_2^{-1}g_1g_2H = g_1H$$

$$g_1^{-1}g_2^{-1}g_1g_2H = H$$

Kako je H grupa, a $e \in H$ imamo $g_1^{-1}g_2^{-1}g_1g_2 \in H$, što važi za sve $g_1, g_2 \in G$.
($\Longleftarrow$) Pretpostavimo da $g_1^{-1}g_2^{-1}g_1g_2 \in H$ za sve $g_1, g_2 \in G$. Neka $g_1H, g_2H \in G/H$. Onda važi $(g_2g_1)^{-1}g_1g_2 \in H$ za sve $g_1, g_2 \in G$. Stoga:

$$g_1g_2H = g_2g_1H$$

odnosno

$$(g_1H)(g_2H) = (g_2H)(g_1H)$$

S obzirom na to da ovo važi za sve $g_1H, g_2H \in G/H$ zaključujemo da je G/H Abelova grupa. ■

Primer 1.2 *U Abelovoj grupi, sve podgrupe su normalne.*

Teorema 1.12 *Neka je $(H, \cdot)$ prava podgrupa grupe $(G, \cdot)$, i neka je $g \in G \setminus H$. Tada je presek skupova H i gH prazan skup.*

Dokaz. Pretpostavimo suprotno, odnosno da postoje elementi h_i i h_j takvi da važi $h_i, h_j \in H$ i $gh_i = h_j$. Ako desno izvršimo operaciju sa obe strane jednakosti sa elementom h_i^{-1} , dobijamo $ge = h_jh_i^{-1}$. Kako važi $h_j \in H$ i $h_i^{-1} \in H$, odavde sledi i da je njihov proizvod u H, odnosno $g \in H$.■

Teorema 1.13 *Ako je $(H, \cdot)$ prava podgrupa grupe $(H, \cdot)$, i $g \in G\setminus H$, onda $|gH| = |H|$.*

Dokaz. Da bi tvrđenje važilo, dovoljno je pokazati da u skupu gH nema duplikata. Pretpostavimo suprotno, odnosno da postoje $h_1, h_2 \in H, h_1 \neq h_2$ takvi da je $gh_1 = gh2$. Ako levo pomnožimo obe strane sa g^{-1}, dobijamo $(g^{-1}g)h_1 = (g^{-1}g)h_2$, odnosno $h_1 = eh_1 = eh_2 = h_2$, što je kontadikcija sa odabirom h_1 i h_2.■

Prethodne dve teoreme nam u većoj meri olakšavaju pokazivanje naredne, izuzetno važne teoreme u teoriji grupa.

Teorema 1.14 *(Lagranž) Ako je $(H, \cdot)$ prava podgrupa konačne grupe $(G, \cdot)$, onda $|H|\,|G|$.*

Dokaz. Odaberimo neki element $g_1 \in G$ takav da g_1 ne pripada skupu H. Ako posmatramo levu klasu g_1H, znamo da važi $|g_1H| = |H|$ na osnovu **Teoreme 1.11**. Sada odaberemo neki drugi element, g_2, koji pripada skupu G, ali ne pripada ni skupu H ni skupu g_1H . Važi $|g_2H| = |H|$, i analogno dokazu **Teoreme 1.10** pokazuje se da je $g_1H \cap g_2H = \varnothing$. Ponovimo postupak formiranja leve klase podgrupe H s obzirom na element koji je u skupu G ali nije u skupu H niti u nekoj od prethodno formiranih klasa onoliko puta koliko je to moguće(dok ne iscrpimo sve takve elemente). Kao rezultat, uspeli smo da pokrijemo ceo skup G levim klasama podgrupe H. Ove klase se ne seku, njihova unija je ceo skup G, a sve imaju istu kardinalnost kao i sam skup H, odakle sledi da je kardinalnost skupa G celobrojni umnožak kardinalnosti skupa H, odnosno $|H|\,|G|$. ■

Napomena: Značaj ove teoreme ogleda se najěšće u problemima pronalaska podgrupa neke zadate grupe. Naime, ukoliko znamo red neke grupe, dovoljno je tražiti njene prave podgrupe među onima čiji je red pravi delilac reda zadate grupe. Treba još napomenuti da obrnuti smer ove teoreme ne važi. Ustaljeni kontraprimer jeste *alternirajuća grupa* reda 12, koja nema nijednu podgrupu reda 6. Međutim, po pitanju obrnutog smera značajan rezultat pružaju teoreme *Silova*

2 Teoreme Silova

Definicija 2.1 *Neka je G konačna grupa takva da važi $|G| = p^k n$, gde je p neki prost broj i ispunjeno je $p \nmid n$. Tada se podgrupa grupe G reda p^k (ukoliko postoji) naziva Silovljevom p-podgrupom.*

Sada je korisno, u cilju dokaza teorema, uvesti definiciju dejstva grupe nad skupom.

Definicija 2.2 *Neka je G grupa i X neprazan skup. Pod dejstvom grupe G na skupu X podrazumeva se homomorfizam $\varphi : G \to S_X$, gde je S_X grupa permutacija skupa X.*

Definicija 2.3 *Neka grupa G dejstvuje na skupom X. Tada orbitu elementa $x \in X$, u oznaci $\Omega(x)$, definišemo kao*

$$\Omega(x) := \{g \cdot x \mid g \in G\}$$

Definicija 2.4 *Neka grupa G dejstvuje na skupu X. Stbilizator elementa $x \in X$ dafinišemo kao*

$$G_x = \{g \in G \mid g \cdot x = x\}$$

Teorema 2.5 *Neka je G grupa reda $p^\alpha m$, gde $m \geq 1$, p prost broj i p ne deli m. Onda:*
(1) Uvek postoji Silovljeva p-podgrupa.
(2) Sve Silovljeve p-podgrupe su međusobno konjugovane.
(3) Broj Silovljevih p-podgrupa je kongruentan sa 1 po modulu p.
(4) Broj Silovljevih p-podgrupa deli red grupe G.

Dokaz.

1. Dokaz izvodimo indukcijom po redu grupe G. Neka je $|G| = n$, i pretpostavimo da tvrđenje važi za svako $k < n$. Razmotrimo dva slučaja:

   (a) Postoji netrivijalna podgrupa H grupe G, takva da $p \nmid [G : H]$. Tada, zbog $|H| < |G|$, važi da H ima Silovljevu p-podgrupu. Kako je $|G| = |H|\,[G : H]$, vidimo da je $v_p(|H|) = v_p(|G|)$, pa je odatle pomenuta Silovljeva p-podgrupa ujedno i p-podgrupa cele grupe G.

   (b) Broj p deli indekse svih podgrupa grupe G. Ukoliko pustimo grupu G da dejstvuje na samu sebe konjugacijom, orbite tog dejstva su konjugovane klase grupe G, a unija jednočlanih orbita će biti centar grupe G. Možemo pisati:

   $$|G| = |Z(G)| + |C_1| + \cdots + |C_k|,$$

   pri čemu je $C_i = \Omega(x_i) = [G : G_{x_i}]$. Odavde vidimo da mora važiti $p \mid |Z(G)|$. Prema Košijevoj teoremi, mora postojati elemenat $x \in Z(G)$ koji je reda p, a pošto taj elemenat x komutira sa svim elementima iz G, $H = \langle x \rangle$ je normalna grupa za koju važi $|G/H| = \frac{n}{p} < n$. Po induktivnoj hipotezi, G/H sadrži Silovljevu p-podgrupu, koju ćemo označiti sa P_0. Ako posmatramo sirjektivni homomorfizam $\pi : G \to G/H, \pi(g) = gH$, znamo da je original

grupe P_0, koji ćemo nazvati P_1, podgrupa od G. Kako je za svako $h \in H$ ispunjeno $hH = H \in P_0$, znamo i da je $H \leq P_1$. Kernel ovog homomorfizma jeste $\ker\pi = P_1 \cap H = H$, te nam Prva teorema o izomorfizmu govori da je $P_1/H \cong P_0$. Konačno,

$$\begin{aligned} &|P_0| = [P_1 : H] = |P_1| \,/\, |H| \\ \implies\ &|P_1| = |P_0|\,|H| = p^{v_p(|G|)} \end{aligned}$$

, odakle vidimo da je P_1 Silovljeva p-podgrupa grupe G. ■

2. Iz prve teoreme, znamo da postoji Silovljeva p-podgrupa, nazovimo je P_1. Neka je $S = \{P_1, P_2, ..., P_k\}$ skup svih različitih konjugata grupe P_1. Najpre ćemo pokazati da $p \nmid k$. Pustimo da G dejstvuje na skup S konjugacijom ($g \cdot P_i = gP_ig^{-1}$). Tada je stabilizator skupa P_i skup $\left\{g \in G \mid gP_ig^{-1} = P_i\right\}$, a ovo je po definiciji normalizator $N_G(P_i)$. Kako su svi P_i konjugati P_1, sledi da imamo samo jednu orbitu (orbita grupe P_1), a to je ceo skup S. Odavde sledi da je $k = |S| = [G : N_G(P_1)]$. Pošto važi $[G : N_G(P_1)] = |G| \,/\, |N_G(P_1)|$, a zbog $P_1 \leq N_G(P_1)$ sledi da je $v_p(|N_G(P_1)|) = v_p(|G|)$, pa u količniku $|G| \,/\, |N_G(P_1)|$ ne postoji faktor p, odnosno $p \nmid k$.
Sada ćemo pokazati da svaka Silovljeva p-podgrupa mora biti sadržana u S. Neka je Q proizvoljna Silovljeva p-podgrupa grupe G i pustimo da ona dejstvuje nad skupom S konjugovanjem. Ovim dejstvom nastaju disjunktne orbite grupa $P_{i1}, P_{i2}, ..., P_{ij}$. Znamo da je:

$$|S| = |\Omega(P_{i1})| + \cdots + |\Omega(P_{ij})|.$$

Po Lagranžovoj teoremi mora biti $|\Omega(P_i)| \mid |Q| = v_p(G) = p^\alpha$, pa je red svake orbite ili 1 ili neki stepen broja p. Kako $p \nmid k$, sigurno postoji bar jedna orbita reda 1. Neka je to orbita P_m. Dakle $1 = |\Omega(P_m)| = [Q : Q_{P_m}]$, gde je $Q_{P_m} = \{g \in Q \mid g \in N_G(P_m)\} = Q \cap N_G(P_m)$. Direktno sledi da je, zbog jednakih kardinalnosti, $Q = Q \cap N_G(P_m)$. Sada, ispunjeno je $P_m \leq N_G(P_m)$, i red faktor grupe $N_G(P_m)/P_m$ nije deljiv sa p, a kako znamo da je i $Q \leq N_G(P_m)$, sledi da možemo ograničiti homomorfizam $\pi : N_G(P_m) \to N_G(P_m)/P_m$ na $\pi : Q \to N_G(P_m)/P_m$. Ovaj novi homomorfizam je zadat sa $\pi(x) = xP_m$. Svaki elemenat grupe Q ima red koji je ili 1 ili neki stepen broja p, dok faktor grupa $N_G(P_m)/P_m$ nema nijedan elemenat reda p, pa se svi elementi grupe Q slikaju u jedinični elemenat grupe $N_G(P_m)/P_m$. To znači da je za svako $x \in G$ ispunjeno $xP_m = P_m$, što je ekvivalnentno sa $x \in P_m$. Sledi da je $Q \leq P_m$, ali zbog $|Q| = |P_m|$ mora biti $Q \cong P_m$, tj. $Q \in S$. ■

3. Neka je $S = \{P_1, \dots P_k\}$. Želimo da pokažemo $|S| \equiv_p 1$.
Pustimo najpre da P_1 dejstvuje nad skupom S konjugacijom. Tada nastaje skup disjunktnih orbita. Primetimo prvo da je $|\Omega(P_1)| = 1$, zbog toga što je $gP_1g^{-1} = P_1$ za sve $g \in P_1$. Dalje, za neko $P_i \neq P_1$ je $|\Omega(P_i)| = [P_1/P_1 \cap N_G(P_i)]$. Analogno dokazu druge Silovljeve teoreme se može pokazati da važi $P_1 \cap N_G(P_i) = P_1 \cap P_i$, te je $|\Omega(P_i)| = [P_1/P_1 \cap P_i]$. Zbog pretpostavke da su P_i i P_1 različite podgrupe,

mora važiti $|P_i \cap P_1| < |P_1|$, odnosno red grupe $P_1/P_1 \cap P_i$ ne može biti 1. Iz razloga što taj red takođe mora deliti $|P_1| = p^\alpha$, vidimo da je red svake orbite Ω_{P_i}, $i = 2, 3, \ldots k$ upravo neki stepen broja p. Ako iskoristimo ovu činjenicu, uviđamo da je

$$|S| = |P_1| + |P_2| + \cdots + |P_k| = 1 + px,$$

što je i trebalo pokazati. ■

4. Primetimo da je dovoljno pokazati da broj Silovljevih p-podgrupa deli red grupe G. Neka je $S = \{P_1, \ldots, P_k\}$ skup svih Silovljevih p-podgrupa. Pustimo G da deluje na elemente skupa S konjugacijom. Pošto su svake dve Silovljeve p-podgrupe konjugovane, znamo da ovim dejstvom nastaje samo jedna orbita. Tada,

$$|S| = |P_1| = [G/N_G(P_1)],$$

a indeks normalizatora podgrupe P_1 deli red grupe G, što je i trebalo pokazati. ■

U cilju provere prostote neke grupe pomoću teorema Silova, posebno je značajna sledeća teorema.

Teorema 2.6 *Ako je Silov p-podgrupa jedinstvena onda je ona i normalna.*

Dokaz. Pretpostavimo da je H jedinstvena Silov p-podgrupa. Za svako $g \in G, gHg^{-1}$ je takođe Silov p-podgrupa jer joj je red isti kao H, a kako je H jedinstvena Silov p-podgrupa, važi $gHg^{-1} = H$. Dakle za svako $h \in H$ važi $ghg^{-1} \in H$ pa je zbog toga H normalna. ■

3 Problem prostote grupe

U ovom poglavlju pokazujemo posledice teorema Silova na primerima rešavanja problema prostote grupa.

Teorema 3.1 *Ne postoji prosta grupa reda pq, gde su p i q različiti neparni prosti brojevi.*

Dokaz. Neka je, bez umanjenja opštosti, $p \leq q$. Ako označimo sa n_q broj Silovljevih q-podgrupa, tada po trećoj Silovljevoj teoremi važi $n_q \mid p$, pa je $n_q \in \{1, p\}$. U slučaju $n_q = 1$, q-podgrupa je jedinstvena i samim tim normalna, dok u slučaju $n_q = p$, znamo $n_q \equiv 1 (mod\ q)$, odakle sledi $p > q$, što je kontradikcija. ■

Teorema 3.2 *Ne postoji prosta grupa reda pq^2, gde su p i q različiti neparni prosti brojevi.*

Dokaz. Posmatraćemo dva slučaja:

1. $p < q$. Označimo sa n_q broj Silovljevih q-podgrupa. Iz $n_q \mid p$ sledi $n_q \in \{1, p\}$.

   (a) $n_q = 1$. Vidimo da je q-podgrupa jedinstvena, odakle je ona i normalna te cela grupa nije prosta.

   (b) $n_q = p$. Sada znamo da je $p \equiv (mod\ q)$, što je kontradikcija sa $p < q$.

2. $p > q$. Ako sada označimo sa n_p broj p-podgrupa, iz $n_p \mid q^2$ sledi $n_p \in \left\{1, q, q^2\right\}$.

   (a) $n_p = 1$. Vidimo da je p-podgrupa jedinstvena, odakle je ona i normalna te cela grupa nije prosta.

   (b) $n_p = q$. Zbog $q \equiv 1(mod\ p)$, nalazimo $q > p$, što je kontradikcija.

3. $n_p = q^2$. Znamo da važi $p \mid q^2 - 1 = (q-1)(q+1)$, a zbog $(q-1, q+1) \leq 2$, mora važiti $p \mid q-1 \veebar p \mid q+1$. Prvi slučaj otpada zbog uslova da je $p > q$. Drugi slučaj je moguć samo kada je $p = q+1$, a u slučaju prostih brojeva je to moguće samo za $p = 2, q = 3$, odnosno red cele grupe G iznosi $2^2 \cdot 3 = 12$. Označimo sada sa n_2 i n_3 redom broj Silovljevih 2-podgrupa i 3-podgrupa. Iz uslova je $n_3 = 4$ a pretpostavićemo da 2-podgrupa nije jedinstvena, tj. da je $n_2 = 3$. Pošto su 3-podgrupe podgrupe prostog reda, znamo da se u preseku svake dve od njih nalazi samo neutralni elemenat, pa u njima ima ukupno $4 \cdot 2 + 1 = 9$ različitih elemenata. Dalje, kako imamo tri 2-podgrupe koje su reda 4, u njihovoj uniji mora biti bar 5 različitih elemenata ne uključujući neutral, te za sada imamo bar $9+5 = 14$ elemenata, a red cele grupe je 12, što dovodi do kontradikcije. ■

Teorema 3.3 *Ne postoji prosta grupa G takva da je $|G| = p^n$, gde je p prost broj i $n \geq 2$.*

Dokaz. Razmotrićemo 2 slučaja:

1. G je Abelova grupa. Pošto $p \mid |G|$, po Košijevoj teoremi postoji elemenat x reda p. Grupa $H = \langle x \rangle$ je reda p pa je ona prava podgrupa grupe G, a kako su u Abelovoj grupi sve podgrupe normalne, vidimo da G nije prosta.

2. G nije Abelova grupa. U tom slučaju, grupa G ima netrivijalni centar, a kako centar predstavlja normalnu podgrupu grupe G, vidimo da ona nije prosta. ■

Teorema 3.4 *Neka je G grupa reda $p^t q$, gde su p i q različiti prosti brojevi takvi da je eksponent t jednak poretku broja p po modulu q. Tada grupa G nije prosta.*

Dokaz. Označimo najpre sa n_p i n_q brojeve Silovljevih p-podgrupa i q-podgrupa. Pošto $n_q \mid p^t$, znamo da je $n_q \in \left\{1, p, p^2, ..., p^t\right\}$, ali zbog uslova $n_q \equiv 1(mod\ q)$ i minimalnosti broja t nalazimo da je n_q jednako 1 ili p^t. Pošto je u slučaju jedinstvenosti q-podgrupe ta podgrupa ujedno i normalna, pretpostavićemo da je $n_q = p^t$. Tada, pošto su sve q-podgrupe prostog reda, presek svake dve od njih čini samo neutral. Dakle, mimo neutrala, postoji ukupno $p^t(q-1)$ različitih elemenata u okviru svih q-podgrupa. Tada je u grupi preostalo još $p^t q - p^t(q-1) = p^t$ elemenata, i oni moraju sačinjavati jedinstvenu p-podgrupu, koja je ujedno i normalna. Odatle sledi da G nije prosta grupa.■

Primedba 3.5 *Prethodnu teoremu možemo blago proširiti i reći da ne postoji prosta grupa G takva da je $|G| = p^k q$, za $k \leq t$.*

Teorema 3.6 *Ako je G grupa i važi $|G| = pq^k$, gde su p i q prosti brojevi takvi da je $p < q$, onda G nije prosta.*

Dokaz. Zbog $q^k \mid\mid |G|$ znamo da postoji Silovljeva q-podgrupa. Označimo sa n_q broj Silovljevih q-podgrupa. Znamo da $n_q \mid p$, pa je $n_q \in \{1, p\}$. Kako mora biti ispunjeno i $n_p \equiv_q 1$, kada bi važilo $n_q = p$ dobili bismo $p > q$, što je kontradikcija. Odavde sledi $n_q = 1$, te je Silovljeva q-podgrupa normalna. ■

Teorema 3.7 *Neka je G grupa i neka je $|G| = p^k n$, gde je p prost broj, $n > 1, k \geq 1$ i važi $|G| > n!$. Tada grupa G nije prosta.*

Dokaz. Neka je H Silovljeva p-podgrupa. Pustimo da G dejstvuje na skup G/H tako da je $g \cdot xH = (gx)H$, za sve $g, x \in G$. Po definiciji, ovo je ekvivalentno sa definisanjem homomorfizma $\varphi : G \to S_n$, tako da je ispunjeno :

$$(\forall g \in G)\varphi(g) = \sigma_g,$$

a σ_g je permutacija zadata sa $\sigma_g(xH) = gxH$. Posmatrajmo sada kernel ovog homomorfizma. Njega čine svi elementi skupa G koji se slikaju u jediničnu permutaciju. Možemo napisati niz ekvivalentnih skupova: $\ker\varphi = \{g \in G \mid \varphi(g) = id\} = \{g \in G \mid gxH = xH\} = \left\{g \in G \mid x^{-1}gxH = H\right\} = \left\{g \in G \mid (\forall x \in G), g \in xHx^{-1}\right\}$. Odavde vidimo da je $\ker\varphi = \bigcap_{x\in G} xHx^{-1}$. Pretpostavimo sada da je kernel homomorfizma φ trivijalan. Razmatramo dva slučaja:

1. $\ker\varphi = \{e\}$. U ovom slučaju znamo da je homomorfizam injektivan, te mora biti $|G| \leq |S_n| = n!$, kontradikcija.

2. $\ker\varphi = G$. U ovom slučaju, dobijamo $|G| = \left|\bigcap_{x\in G} xHx^{-1}\right| \leq |H|$, što je kontradikcija jer je H podgrupa G.

Dakle, došli smo u kontradikciju sa pretpostavkom, pa $\ker\varphi$ čini netrivijalnu normalnu podgrupu grupe G. ■

Literatura

[1] Božović, N., Mijajlović, Ž., *Uvod u teoriju grupa*, Naučna knjiga, Beograd, 1990.

[2] Dolinka, I. , *Predavanja iz teorije grupa*, Prirodno matematički fakultet, Univerzitet u Novom Sadu, 2018.

[3] Lee, G. T. , *Abstract Algebra - an introductory course*, Department of Mathematical Sciences, Lakehead University,2018.

[4] Petrović, Z. , *Algebra 1 - predavanja za školsku 2014/15 godinu*, Matematički fakultet, Univerzitet u Beogradu, 2014.

[5] Petrović, Z. , *Algebra 2 - predavanja za školsku 2014/15 godinu*, Matematički fakultet, Univerzitet u Beogradu, 2014.

[6] *Notes on Sylow's theorems*, https://math.berkeley.edu/ kpmann/SylowNotes.pdf

[7] *4 ways to show a group is not simple*, 4.5.2015.,
https://www.math3ma.com/blog/4-ways-to-show-a-group-is-not-simple